REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
2/6/08

2. REPORT TYPE
Final Report

3. DATES COVERED *(From - To)*
3/15/2004 - 6/30/2007

4. TITLE AND SUBTITLE
UC Davis Center for Digital Security

5a. CONTRACT NUMBER

5b. GRANT NUMBER
FA9550-04-1-0171

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
DM Rocke, NG Jensen, G Rodrigue, BH Kolner, DL Woodruff, R Vemuri

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Regents of the University of California
University of California,
Davis, Sponsored Programs
1850 Research Park Drive,
Suite 300
Davis, CA 95618

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
USAF,AFRL
AF Office of Scientific/NL
Research
875 Randolph Street, Rm. 3112
Arlington, Virginia 22203

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-SR-AR-TR-08-0098

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Approved for Public release

20100916262

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The UC Davis Center for Digital Security is based on the premise that long-range research requires unconventional approaches. In this report of our activities under this grant, we outline the accomplishments of the main working groups in our Center. This includes the following

1. Josephson Devices for Quantum Information Processing (page 1).
2. Modeling Communication Losses and Interference in Fiber Optic Systems (page 9).
3. Low Detectability Optical Code-Division Multiple Access Communications on a Broadband WDM Network (page 16).
4. Network Interdiction (page 24).
5. Intrusion Detection (page 26).

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			DM Rocke
				29	19b. TELEPHONE NUMBER *(include area code)* (530) 752-6999

DTIC Data

Purchase Request Number: FQ8671-0600473

BPN: F1ATA05258B473

Proposal Number: 04-NM-045

Research Title: UC DAVIS CENTER FOR DIGITAL SECURITY

Type Submission: Final

Inst. Control Number: FA9550-04-1-0171P00002

Institution: UNIV OF CALIFORNIA, DAVIS

Primary Investigator: Dr. David Rocke

Invention Ind: none

Project/Task: 2304F / X

Program Manager: Dr. Robert L. Herklotz

Objective:

To continue the UC Davis Center for Digital Security (CDS). The purpose of the center is to investigate vulnerabilities in computers, networks, optical and electrical transmission of information, wireless transmission of information, power generation and transmission, and other related areas and to help develop methods of protection against these emerging threats to military and commercial communication and computation.

Approach:

To address a broader array of potential vulnerabilities and methods of attack and protection than is typical in computer security research. In addition to areas such as intrusion detection, encryption, authentication, certification, and so forth, we intend to address physical as well as electronic security issues such as network interdiction, physical data encoding, modeling and simulation of methods of physical inference and information gathering, etc. At all times, CDS will stress flexibility and agility in its approaches to these and other problems in order to cope effectively with the fast-paced advances in the underlying technologies. We will also fully exploit the Department of Applied Science's world-renowned strengths in applied physics to investigate security issues in, for example, optical networking as this technology gradually and ubiquitously supplants much of the world's previously electronics-based computing and communications infrastructure.

Progress:

Year: 2003 **Month:**

NONE REQUIRED AT THIS TIME.

Year: 2004 **Month:** 11

ANNUAL REPORT FOR: FA9550-04-1-0171

The accurate characterization of signal loss is a valuable measure of the reliability of communication systems. This is particularly important in light-wave communication systems where wave attenuation and alteration limits the performance of the optical fiber as a data transmission channel. These unwanted signal modifications can occur from a variety of sources. Intrinsic glass manufacturing inconsistencies can cause wave attenuation through the scattering and absorption of light energy. Attenuation from these sources is dependent on the material of the particular optical fiber. Wave alterations from external sources are more difficult to characterize as they can arise from factors such as mechanical deformations of the fiber such as bends or electromagnetic effects such as electrical fields. Consequently, a better understanding of these losses will lead to more efficient optical communication systems.

Progress:

Year: 2005 **Month:** 11

Annual Report for FA9550-04-1-0171

The past year's activity on the Josephson junction project has been devoted to analyzing several essential details of experimental observations, and to put these observations in the context of the possibilities for using Josephson junctions for quantum computing and quantum information processing. The bulk part of the work within the AFOSR project is purely theoretical and colnputational, but the effort connects closely to the general literature on extreme low temperature measurements on Josephson systems, and, in particular, to measurements being performed in the experimental laboratories of our collaborators in Rome, Italy.

Year: 2006 **Month:** 09

The principle of Code-Division-Multiple-Access applied in the wavelength domain is an attractive venue for applying secure communications techniques. An eavesdropper listening in on an O-CDMA channe without prior knowledge of which particular orthogonal code group is being used must search with exponential time to decipher a message.

Year: 2008 **Month:** 02 **Final**

The UC Davis Center for Digital Security is based on the premise that long-range research requires unconventional approaches. In this report of our activities under this grant, we outline the accomplishments of the main working groups in our Center. This includes the following

1. Josephson Devices for Quantum Information Processing (page 1).
2. Modeling Communication Losses and Interference in Fiber Optic Systems (page 9).
3. Low Detectability Optical Code-Division Multiple Access Communications on a Broadband WDM Network (page 16).
4. Network Interdiction (page 24).
5. Intrusion Detection (page 26).

Center for Digital Security
University of California, Davis

David M. Rocke, PI

AFOSR Agreement Number FA9550-04-1-0171

Final Report

January 2008

Overview

The UC Davis Center for Digital Security is based on the premise that long-range research requires unconventional approaches. In this report of our activities under this grant, we outline the accomplishments of the main working groups in our Center. This includes the following

1. Josephson Devices for Quantum Information Processing (page 1).
2. Modeling Communication Losses and Interference in Fiber Optic Systems (page 9).
3. Low Detectability Optical Code-Division Multiple Access Communications on a Broadband WDM Network (page 16).
4. Network Interdiction (page 24).
5. Intrusion Detection (page 26).

Progress report, Fall 2005, for the Josephson junction project

(an analysis of Josephson devices for quantum information processing)

Niels Grønbech-Jensen

Department of Applied Science, University of California, Davis, California 95616

(Dated: October 20, 2005)

Abstract

The past year's activity on the Josephson junction project has been devoted to analyzing several essential details of experimental observations, and to put these observations in the context of the possibilities for using Josephson junctions for quantum computing and quantum information processing. The bulk part of the work within the AFOSR project is purely theoretical and computational, but the effort connects closely to the general literature on extreme low temperature measurements on Josephson systems, and, in particular, to measurements being performed in the experimental laboratories of our collaborators in Rome, Italy.

Since 1985, when observations of macroscopic quantum behavior in large area Josephson junctions were reported, many experimental observations have been reported by different research groups showing ever sophisticated measurements showing signatures that are generally attributed to quantization of the Josephson phase. However, direct observation of the quantum state has not been accomplished. Instead, the extracted information is inferred through macroscopic manipulations that produce indirect signatures, which are then interpreted. It is the purpose of this project to investigate these measurements in light of a purely classical model, thereby cast the problem in a convenient theoretical framework, which can be mathematically tackled, and which may provide plausible alternative interpretations of the experimental observations. Through this work, we hope to generate a deeper understanding of the differences and similarities between classical and quantum mechanical observables in nonlinear systems. We also believe this work will produce new suggestions for insightful experimental measurements that can shed light on the nature of the Josephson device and its device physics.

I. INTRODUCTION

Much experimental attention has recently been given to the topic of Rabi-oscillations [1] in microwave irradiated Josephson systems at very low temperatures [2–5]. A common motivation for the studies is the proposed macroscopic quantum behavior outlined in Ref. [6], which has opened the way for potential applications of Josephson technology in quantum information processing [7]. This is proposed by operating a Josephson junction in its zero-voltage state at temperatures below the quantum transition temperature, while manipulating the possible energy states with the application of commensurate microwave frequencies. The significance of Rabi-oscillations is many fold, and includes *i*) a direct connection to a well known quantum mechanical concept in perturbed atomic systems, and *ii*) a method by which the control of quantum states of a system can be evaluated. Thus, it is of significant importance to understand the nature of these observations in order for us to evaluate how to interpret the Josephson system under investigation.

Recent classical analyses of Josephson junctions, perturbed by microwaves and low temperature thermal fluctuations, have revealed that key signatures [8–10], used to display quantum mechanical features of Josephson junctions, have direct classical analogs, which may obscure the interpretation of the observations [11–13]. Inspired by the work on slowly modulated transients to phase-locking in Josephson systems by Lomdahl and Samuelsen [14], we have most recently demonstrated [15, 16] that also Rabi-oscillations have a classical analogue in microwave perturbed Josephson junctions, providing a system response very similar to the reported observations under the same conditions. Thus, we are now faced with the questions of how to interpret the experimental measurements, and how to explore more telling signatures that can clearly distinguish between classical and quantum mechanical behavior.

II. CLASSICAL MODEL

A normalized classical equation for a Josephson junction can be written [17]

$$\ddot{\varphi} + \alpha\dot{\varphi} + \sin\varphi \;=\; \eta + \varepsilon_s(t)\sin(\omega_s t + \theta_s) + \varepsilon_p(t) + n(t) \;, \qquad (1)$$

where φ is the difference between the phases of the quantum mechanical wave functions defining the junction, η represents the dc bias current, and $\varepsilon_s(t)$ and ω_s represent microwave

current amplitude and frequency, respectively. All currents are normalized to the critical current I_c, and time is measured in units of the inverse plasma frequency ω_0^{-1}, where $\omega_0^2 = 2eI_c/\hbar C = 2\pi I_c/\Phi_0 C$, C being the capacitance of the junction and $\Phi_0 = h/2e$ the flux quantum. The phase of the applied microwave field is θ_s. Tunneling of quasiparticles is phenomenologically represented by the dissipative term, where $\alpha = \hbar\omega_0/2eRI_c$ is given by the shunt resistance R, and the accompanying thermal fluctuations are defined by the dissipation-fluctuation relationship [18] in which the thermal energy k_BT is normalized to the characteristic Josephson energy $H_J = I_c\Phi_0/2\pi$. A current pulse for probing the state of the system is represented by $\varepsilon_p(t)$.

From the above normalizations, we define the normalized energy from the time independent perturbation terms in Equation (1)

$$H = \frac{1}{2}\dot{\varphi}^2 + 1 - \cos\varphi - \eta\varphi \,. \tag{2}$$

The undamped bias current dependent plasma frequency is given by

$$\omega_J = \sqrt[4]{1-\eta^2} \,. \tag{3}$$

Within this widely used and well accepted classical model, we have made analyses and conduct simulations according to experiments reported in, e.g., Refs. [2, 5]. System parameters, such as η, α, ω_s, $\varepsilon_s(t)$, and $\varepsilon_p(t)$ are matched as closely as possible to experimentally reported values.

III. ACCOMPLISHMENTS

Rabi-type Oscillations: We have demonstrated the surprising result that classical Rabi-type oscillations are indeed observed statistically through simulations of the distribution of probe field induced switching from the zero-voltage state as a function of applied microwave field $\varepsilon_s(t)\sin(\omega_s t + \theta_s)$. The initial result has been published in Ref. [15], where the experimental recipe described in the experimental paper [2] was followed. The paper not only numerically demonstrated that the phenomenon of Rabi-type oscillations is present in the classical system, but also provided a complete analytical reasoning based on detailed perturbation analysis of the theoretical model. This analysis provides both an intuitive (and simple) reasoning for the classical oscillations and it provides *quantitative* predictions for the observed Rabi-type frequency,

since the theory depends entirely on experimental parameters that are not fitted. This work has caught quite a bit of interest, resulting in several invited presentations at international conferences/workshops where the prospect of Josephson applications in quantum information processing is discussed.

A couple of important features were missing from the theory presented in Ref. [15], such as the inclusion of damping. Also, the results could not be put in closed analytical form, which is obviously desirable. As a result, we decided to develop a new, complementing, theory of the phenomenon. This is presented in Ref. [16], where a perturbation theory is based on the dynamical variables instead of the system energy, as was done in Ref. [15]. This allows for both closed form predictions of the Rabi-type frequency *and* for the inclusion of dissipation, which results in the classical equivalent of the experimentally observed coherence time. In addition to developing this new expanded theory, which gives results similar to those found in Ref. [15], we decided to also test another experimentally reported experimental procedure for observing Rabi-oscillations in Josephson systems. The *quantitative* comparison between our theory and the reported results is nearly perfect (see Ref. [16]).

These results, which have come to the community as somewhat of a surprise, tell us several valuable things. First, the experimental observables are not unique to quantum mechanics, and a classical analysis is indeed sufficient to describe the observations. Second, while it is very difficult to formulate and solve a complete quantum mechanical theory for Rabi-oscillations in driven, damped Josephson systems, a classical theory will provide several key predictions that can guide further experiments, such as give the Rabi-type frequency and decay time as a function of known system parameters. Third, our results have provided increased activity for identifying experiments that will indeed demonstrate unambiguous signatures of quantum mechanical features.

Multi-Peak Switching Distributions: We have investigated, experimentally, numerically, and theoretically a more complicated system consisting of two Josephson junctions in a superconducting loop (a Superconducting Interferometer) [19]. The objective is to evaluate if multi-peak switching distributions, which are observed in Josephson systems at very low temperatures when resonant microwave radiation is applied to the system, are due to classical nonlinear dynamics or due to quantum mechanical effects.

This particular system of more than one junction is also an avenue for probing systems that represent application circuits instead of single devices, and it introduces to the model another experimentally important parameter, magnetic flux, which can be used to manipulate a system. As we previously have demonstrated for single Josephson junctions, this system responds in its switching statistics to microwaves with multi-peak distributions, and the anomalous distributions can be reproduced within the classical model. Further, the results are compared directly to matching experiments conducted above, but close to, the so-called quantum transition temperature.

Thus, we have provided direct evidence of classical behavior being consistent with experimental observations that have previously been attributed to signatures of quantum behavior.

New Preliminary Work: We have just completed (no yet submitted) a simulation study of the effects of temperature and dissipation on the experimentally observed features. This study indicates that reported observations are consistent (nothing inconsistent has yet been found) with the classical model.

We are working on an investigation of controlling the phase of the applied microwave radiation. The significance of this study is, first, that while such control is within reach of experiments, observations have not yet been reported, and we can therefore provide true predictions that may (or may not) be validated. Second, as preliminary studies suggest that additional system control can be gained by controlling this phase, we hope this work will contribute additional significant value to the potential of Josephson technology.

IV. LESSONS AND FUTURE WORK

The consistency between the classical model and analysis with experimental observations lends credibility to the value of a classical interpretation of, e.g., the reported Rabi-oscillations, since the quantum mechanical and classical intuition turns out to be very similar:

The macroscopic quantum picture interprets the observed oscillations as a result of a microwave induced temporal variation in the population probability of two, or more, intrinsic quantum mechanical energy levels in the Josephson washboard potential. This

slow variation is then indirectly observed through the associated variation in tunneling probability, switching from the zero-voltage state as a result of the application of the probe pulse. The stochastic nature of the system is due to the absorption of microwave photons as well as the subsequent tunneling probability of the measurement.

The classical picture presents a system with a microwave induced temporally modulated energy. The slow variation is indirectly observed through the associated variation in escape from the energy well when the probe is applied, with high probability for passing the energetic saddle point during times of elevated energy and relatively little escape probability during times of depressed energy content. The stochastic nature of this system is due to the random phase of the microwave signal as well as the thermal fluctuations.

Additional analogies between intrinsic quantum mechanical energy levels and the multi-valued resonances of the classical nonlinear system briefly outlined above and in our cited work further bridges the gap between what can be expected from the two interpretations of the microwave induced measurements. Since the experimental measurements are concerned only with detecting the escape event, and since the classical and quantum mechanical interpretations seem to provide the same signatures for that escape, we are faced with a fundamental ambiguity of how to read this information. Potential applications of Josephson technology for quantum information processing will therefore benefit from the development of new unambiguous measurements, which must present signatures of macroscopic quantum behavior that cannot be explained classically. Only a close synergy between experiment and theory can achieve this goal, since the theoretical model can be formulated purely classical, thereby eliminate any doubt as to the origin of various observations. We are therefore enthusiastically continuing our explorations in order to understand observed features, such as Ramsey fringes, as well as suggesting specific experiments that can resolve and promote this very important scientific problem in quantum information processing.

A specific emerging idea from our work is that resolving the question of whether or not an observed phenomenon is classical or quantum mechanical must be understood *without* application of microwaves, and possibly without using the switching events as core measurements. The reason is that the application of microwaves induces resonant states in the classical system that mimic the energy quantization of the corresponding quantum mechan-

ical description. The measurement of switching events seems considerably removed from the physics of interest since the measurement of the switching event happens *after* the possible quantum state of interest has been destroyed. These are direct clues to new suggestions for experiments.

V. AFOSR PUBLICATIONS AND SIGNIFICANT PRESENTATIONS

1. *Rabi-type oscillations in a classical Josephson junction*, Ref. [15] (Attached)
2. *Classical analysis of phase-locking transients and Rabi-type oscillations in microwave-driven Josephson junctions*, Ref. [16] (Attached)
3. *Investigation of Josephson interferometer potentials by ac excitations*, Ref. [19] (Attached)
4. Invited Speaker, "Problemi Attuali di Fisica Teorica – Meccanica Quantistica e Computazione Quantistica", Vietri sul Mare (Italy), Friday 18 - Sunday 20 March 2005.
   Title: **Rabi-type oscillations in a classical Josephson junction.**
5. Invited Speaker, "New Trends in Quantum Mechanics: Fundamental Aspects and Applications" (Quantum Devices), Grand Hotel et des Palmes, Palermo, Italy, November 11-13, 2005.
   Title: **Classical interpretation of anomalous modulations in the escape statistics of low temperature Josephson junctions.**

Our experimental collaborators in Rome, Italy, are supported by MIUR (Italy) COFIN04.

---

[1] I. I. Rabi, Phys. Rev. **51**, 652 (1937).

[2] J. M. Martinis, S. Nam, and J. Aumentado, Phys. Rev. Lett. **89**, 117901 (2002).

[3] A. J. Berkley, H. Xu, M. A. Gubrud, R. C. Ramos, J. R. Anderson, C. J. Lobb, and F. C. Wellstood, Phys. Rev. B **68**, 060502 (2003).

[4] R. W. Simmonds, K. M. Lang, D. A. Hite, S. Nam, D. P. Pappas, and John M. Martinis, Phys. Rev. Lett. **93**, 077003 (2004).

[5] J. Claudon, F. Balestro, F. W. J. Hekking, and O. Buisson, Phys. Rev. Lett. **93**, 187003 (2004).

[6] A. O. Caldeira and A. J. Leggett, Phys. Rev. Lett. **46**, 211 (1981).

[7] *Quantum Computing and Quantum Bits in Mesoscopic Systems*, A. Leggett, B. Ruggiero, and P. Silvestrini Eds. (Kluwer Academic/Plenum Publishers, New York, 2004).

[8] J. M. Martinis, M. H. Devoret, J. Clarke, Phys. Rev. Lett. **55**, 1543 (1985).

[9] A. Wallraff, T. Duty, A. Lukashenko, and A. V. Ustinov, Phys. Rev. Lett. **90**, 037003 (2003).

[10] A. Wallraff, A. Lukashenko, J. Lisenfeld, A. Kemp, M. V. Fistul, Y. Koval, and A. V. Ustinov, NATURE (London) **425**, 155 (2003).

[11] N. Grønbech-Jensen, M. G. Castellano, F. Chiarello, M. Cirillo, C. Cosmelli, L. V. Filippenko, R. Russo, and G. Torrioli, Phys. Rev. Lett. **93**, 107002 (2004).

[12] N. Grønbech-Jensen, M. G. Castellano, F. Chiarello, M. Cirillo, C. Cosmelli, V. Merlo, R. Russo, and G. Torrioli, in "Quantum Computing: Solid State Systems", edited by B. Ruggierio, P. Delsing, C. Granata, Y. Paskin, and P. Silvestrini (Kluwer Academic and Springer Publishers, New York, to be published), cond-mat/0412692.

[13] N. Grønbech-Jensen and M. Cirillo, Phys. Rev. B **70**, 214507 (2004).

[14] P. S. Lomdahl and M.R. Samuelsen, Phys. Lett. A **128**, 427 (1988); N. Grønbech-Jensen, Y. N. Kivshar, and M. R. Samuelsen, Phys. Rev. B **47**, 5013 (1993).

[15] N. Grønbech-Jensen and M. Cirillo, Phys. Rev. Lett. **95**, 067001 (2005).

[16] Jeffrey E. Marchese, Matteo Cirillo, and N. Grønbech-Jensen, Submitted to Physical Review B (2005) [cond-mat/0509729].

[17] A. Barone and G.釣Paternó, *Physics and Applications of the Josephson Effect* (Wiley, New York, 1982); T. Van Duzer and C. W. Turner, *Principles of Superconductive Devices and Circuits* , 2nd ed.(Prentice-Hall, New York, 1998).

[18] G. Parisi, *Statistical Field Theory* (Addison-Wesley, Redding, MA, 1988).

[19] M. Cirillo, P. Carelli, M. G. Castellano, F. Chiarello, C. Cosmelli, N. Grønbech-Jensen, R. Leoni, J. E. Marchese, F. Mattioli, G. Torrioli, and D. Simeoni, Submitted to Physica C (2005).

Project Title : Modeling Communication Losses and Interference in Fiber Optic Systems

Principal Investigator : Garry Rodrigue

Philosophy : **The accurate characterization of signal loss is a valuable measure of the reliability of communication systems. This is particularly important in lightwave communication systems where wave attenuation and alteration limits the performance of the optical fiber as a data transmission channel. These unwanted signal modifications can occur from a variety of sources. Intrinsic glass manufacturing inconsistencies can cause wave attenuation through the scattering and absorption of light energy. Attenuation from these sources is dependent on the material of the particular optical fiber. Wave alterations from external sources are more difficult to characterize as they can arise from factors such as mechanical deformations of the fiber such as bends or electromagnetic effects such as electrical fields. Consequently, a better understanding of these losses will lead to more efficient optical communication systems.**

Methodology: Numerical simulation is used to study the losses in optical fibers incurred by external factors. The underlying model is the nonlinear vector wave equation

$$\varepsilon \frac{\partial^2 \vec{E}}{\partial t^2} = \nabla^2 \vec{E} - \frac{\partial^2 \vec{P}}{\partial t^2}$$

The Galerkin method provides the numerical approximation

$$\tilde{E}(\vec{x},t) = \sum_{j=1}^{N} e_j(t) \vec{W}(\vec{x})$$

where $\vec{W}_1, \vec{W}_2, \ldots, \vec{W}_N$ are vector polynomials. Propagating modes that satisfy the above nonlinear wave equation must be tangentially continuous across interfaces and numerical approximations must do the same. This is accomplished by using Whitney edge elements as the vector polynomial basis functions $\vec{W}_i$.

Accomplishments (2004/2005)

I. High Order Vector Finite Element Method

A high order vector finite element method for solving Maxwell's equations was developed. The method has several key benefits. High order spatial discretizations are achieved by employing high order interpolatory basis functions derived from the Nedelec polynomial spaces. These properly model the jump discontinuities of field intensities and flux densities across material interfaces and maintain charge conservation. High order temporal discretization is achieved via symplectic integration methods. It is now possible to simulate longer fibers, cf. Fig. 1

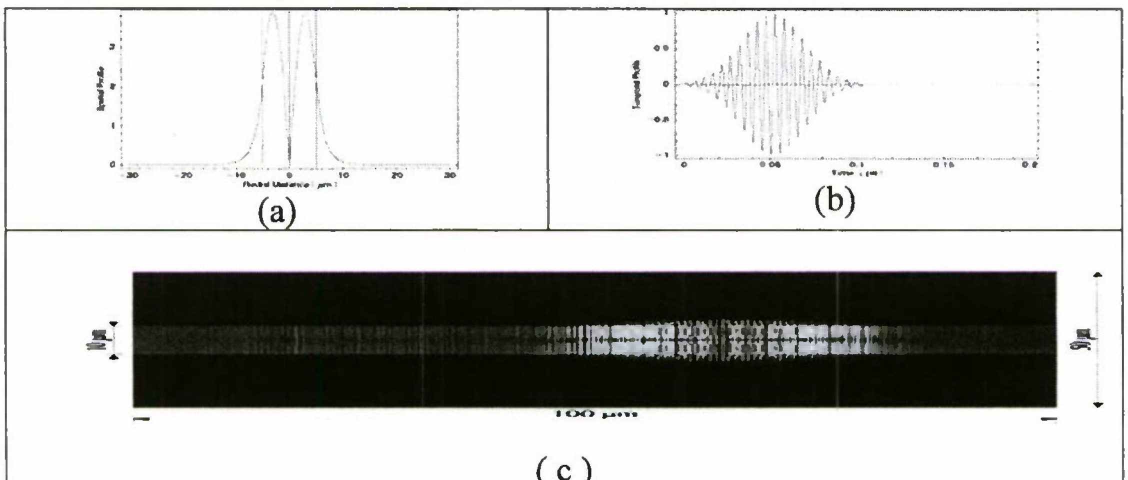


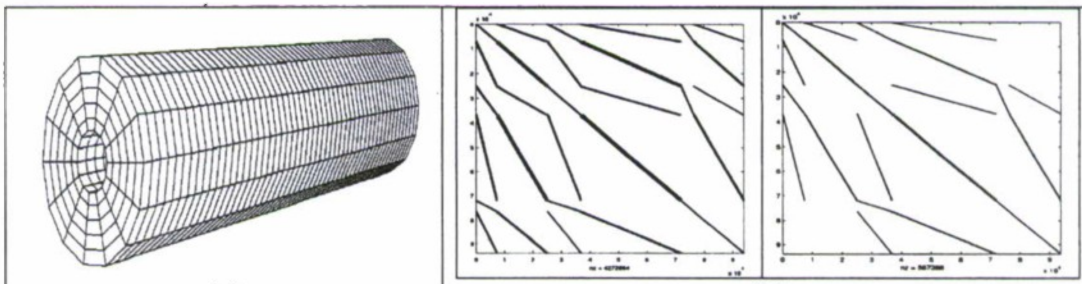
Figure 1: (a) Spatial and (b) temporal profile of pulsed voltage to excite fiber;(c) Snapshot of electric field magnitude using third order polynomials

II. Mass Lumping

Time domain vector finite element solutions of Maxwell's equations require the solution of a sparse linear system involving the mass matrix

at every time step. This process represents the bulk of the computational effort in time dependent simulations. As such, mass lumping technique in which the mass matrix is reduced to a diagonal or block-diagonal is desirable. A special set of high order curl-conforming basis functions and reduced order integration rules has been developed which allow for a dramatic reduction in the number of non-zero entries in a vector finite element mass matrix. The method is derived from the Nedelec curl-conforming polynomial spaces and is valid for arbitrary order hexahedral basis functions for finite element solutions to the second order wave equation for the electric (or magnetic) field intensity.

To get a sense of the computational savings achieved by the new mass lumping scheme, a simple coaxial cable signal propagation was performed. In this experiment 2nd order basis functions were used and the mass lumping scheme was compared to the non-mass lumped scheme,cf. Fig.2,3.



(a) (b)

Figure 2 (a) Mesh representing coaxial cable (b) Sparsity plots of cable mass matrices using full integration (right) and mass lumping (left)

	Full Integration	Mass Lumping
No. Unknowns	93,772	93,722
No. Timesteps	2,000	1,000
No. Conj. Grad. Iterations / Timestep	43	10
Avg. CPU time / Timestep	3.36 s	0.94 s

(a)

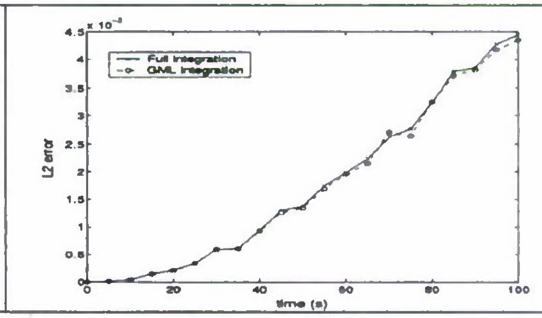


Figure 3 (a) Comparison of cost for Coax simulation with full integration method and the Generalized Mass Lumping (GML) scheme (b) L2 error between full integration method and GML method

III. Bent Step-Indexed Fiber

Local bending of an optical fiber can change the refractive properties of the fiber so that light energy is radiated away from the guiding directions and power loss occurs. A TE01 mode was propagated in a step-indexed bent optical fiber of varying curvature radii and bend angles to determine the resulting power loss in the core, cf. Fig. 4,5.

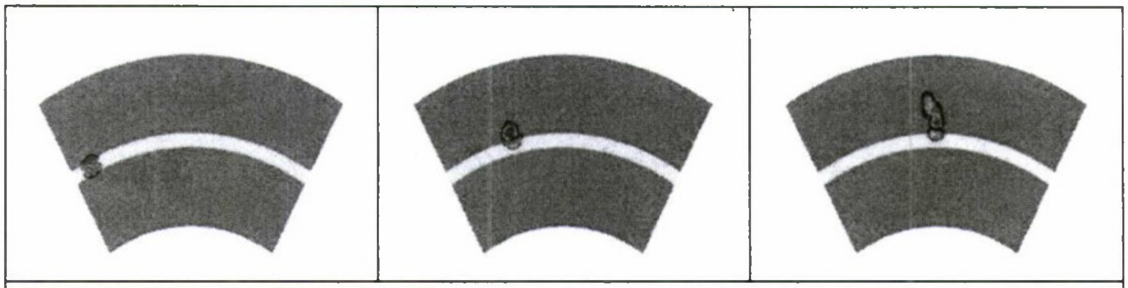


Figure 4 : Three different shapshots of the electric field intensity

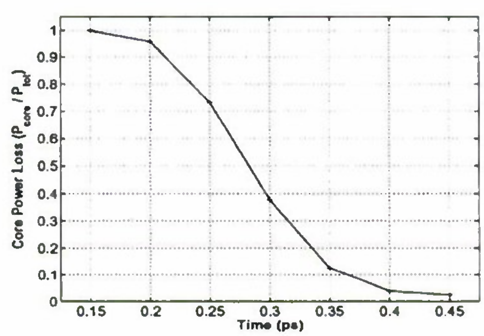
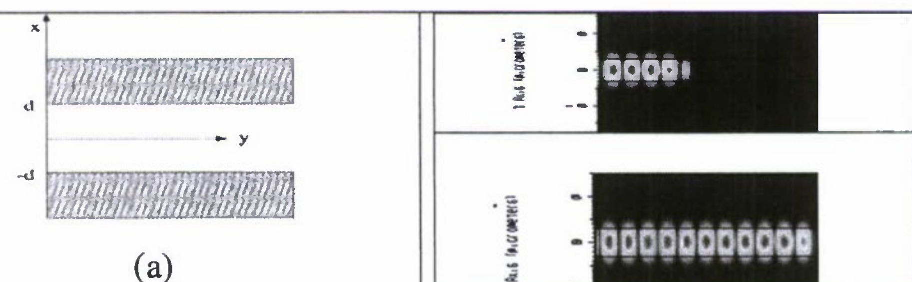


Figure 5 :Relative core power loss as a function of time for a bent optical fiber simulation

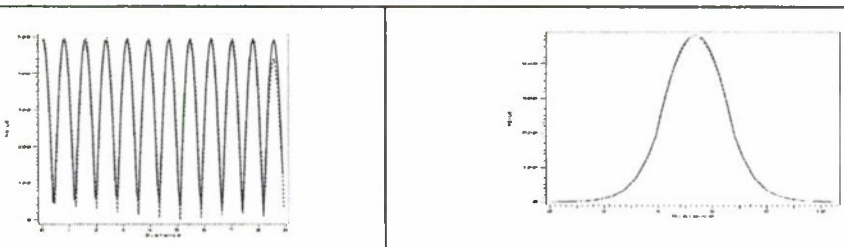
IV. External Fields

Changes in the refractive index of a material can be induced by the application of an external electric field. The presence of such a field distorts the crystal structure so that changes in the optical properties occur and is known as the Kerr effect. The refractive index in this case is given by $n_0 + n_2|E|^2$, where the total refractive index consists of the linear refractive index n_0 and an added effect due to the intensity of an externally applied field with n_2 as the Kerr coefficient of the material. A new numerical technique was developed to solve the nonlinear Kerr-Maxwell equations. A singular perturbation was applied to the nonlinear Maxwell equations to generate two linear equations which are then numerically solved by out existing vector finite element method. The numerical technique was verified on a two-dimensional rectangular waveguide where the exact solutions were known, cf. Fig. 6,7.



(a) (b)

Figure 6 :(a) Geometry of 3-layer optical guide with linear core and nonlinear cladding, (b) TE0 mode propagation at t = 2.52 ns (top) and 7.1 ns (bottom)



(a) (b)

Figure 7 :(a) TE0 mode computation between exact and computed solution at t = 7.1 ns and (b) y = 7 microns

V. Publications

1. High order symplectic integration methods for finite element solutions to time dependent Maxwell equations , with R. Rieben and D. White, IEEE Trans. Ant. Prop., vol. 52, pp. 2190-2195, 2004
1. A high order mixed vector finite element method for solving the time dependent Maxwell equations on unstructured grids, with R. Rieben and D. White, in press, J. of Comp. Physics
2. A generalized mass lumping techniques for vector finite element solutions of the time dependent Maxwell equations, with A. Fisher, R. Rieben, and D. White, submitted IEEE Trans. Ant. Prop.
3. Propagation of weakly guided waves in a Kerr nonlinear medium using a perturbation approach, with J. Mariani, submitted J. of Lightwave Technology
4. Vector finite element modeling of the full-wave Maxwell Equation to evaluate power loss in bent optical fibers, submitted J. of Lightwave Technology
5. A reduced integration techniques for generalized mass lumping in finite solutions of the time dependent Maxwell equations, with A. Fisher, R. Rieben and D. White, Proc. of IEEE Ant. and Prop. Soc., Monterey,CA, June 20-26,2004
6. Application of a novel high order time domain vector finite element method to photonic band-gap waveguides, with R. Rieben and D. White, Proc. of IEEE Ant. and Prop. Soc., Monterey,CA, June 20-26,2004

VI. Personnel Supported

Jennifer Dacles-Mariani : Postgraduate Researcher

LOW DETECTABILITY OPTICAL CODE-DIVISION MULTIPLE ACCESS COMMUNICATIONS ON A BROADBAND WDM NETWORK.

Professor Brian H. Kolner, Department of Applied Science

Introduction

This year saw continued progress in the development of our prototype Optical Code-Division Multiple Access (OCDMA) fiber-optic communications system. The goal of this system is to allow multiple users to share the same optical fiber and overlap in physical space (spatial modes), time, and wavelength. In addition, this system will allow for straightforward inclusion of coded access both at the transmitter and receiver, which is a very desirable feature for secure data transmission.

The OCDMA program at UC Davis is supported by both the AFOSR and DARPA and involves six faculty and up to 12 students and post-docs. It is a multidisciplinary project involving optical hardware design, coding and information theory, and integrated optics design and fabrication for microscale deployment of OCDMA technology.

The principle of OCDMA is based on applying a phase code across the spectrum of a femtosecond optical pulse. The code is bilevel (0 or π) and is applied with a liquid-crystal light modulator which follows a diffraction grating. Figure 1 shows a pictorial view of an encoder/decoder set up to process five simultaneous data streams. Data from optical fibers pass through a circulator which is a three-port device that routes the signals from port-to-port in a counterclockwise fashion. The light comes out of the circulator and into a collimator which converts the fiber-bound signal to a free-space optical wavefront. A pair of cylindrical lenses acts as a one-dimensional telescope to broaden the beam so that it is uniformly spread out on the face of the diffraction grating (thus maximizing the number of grooves that are illuminated). The diffracting grating then spreads out the wavelength spectrum into the transverse plane where it impinges on the two dimensional liquid-crystal spatial-light phase-modulator (2D LC-SLPM). This is a reflection-mode device and thus the wavefront is reflected back along its incident path. We chose to use a two-dimensional LC-SLPM as a cost-savings measure since it can accommodate up to five simultaneous users. The LC-SLPM is pixilated into an array of 768x768 elements, each of which is individually addressable with uniform phase shift from 0 to a little over 2π radians. The array is divided into 5 sub-array sections, each one 154x768 pixels. The codes are written into this sub-array as a 1x64 chip phase map. Since the wavelengths are spread horizontally there is no need to have any vertical coding. Implementing a uniform coding scheme would require that each chip in the code use 768/64=120 elements. However, since the power spectrum of our femtosecond light pulses is roughly hyperbolic-secant in shape, we discovered that it is more effective to use a nonuniform coding. That is, the chip size is increased in the wings of the spectrum where the energy is reduced. This was found to improve (lower) the bit-error-rate (BER). Figures 2-4 show the spectrum of our modelocked laser pulse with no coding (Fig. 2), a 31-bit M-sequence code (Fig. 5) and a 64-bit Walsh code applied (Fig. 4).

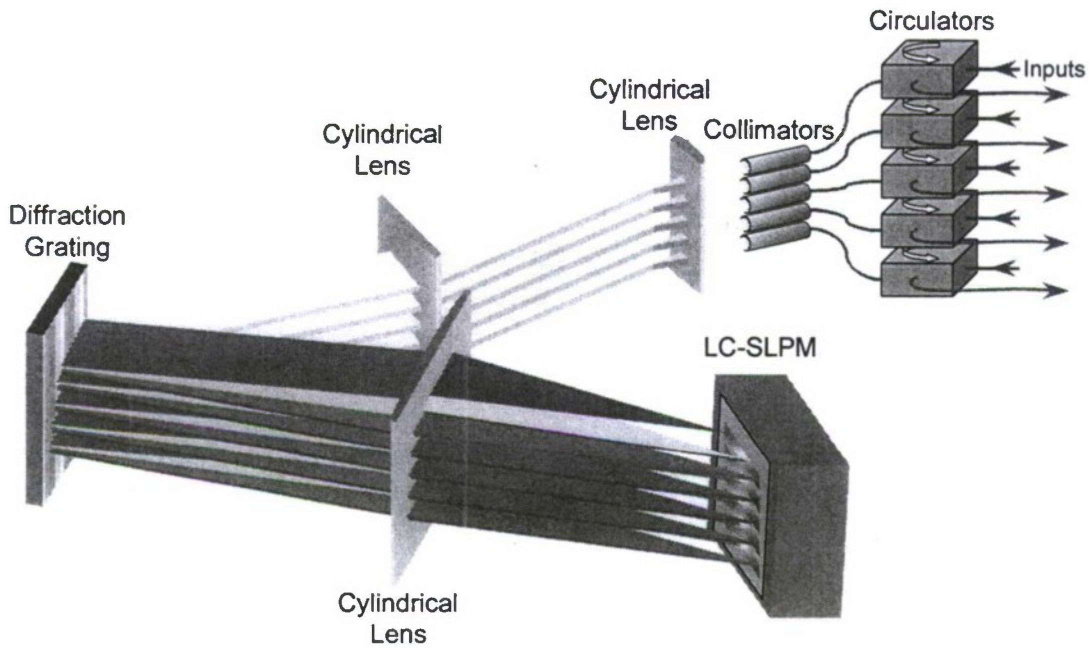


Figure 1. Pictorial view of the two-dimensional liquid-crystal spatial light phase modulator (2-D LC-SLPM) showing how it is used to encode or decode multiple channels.

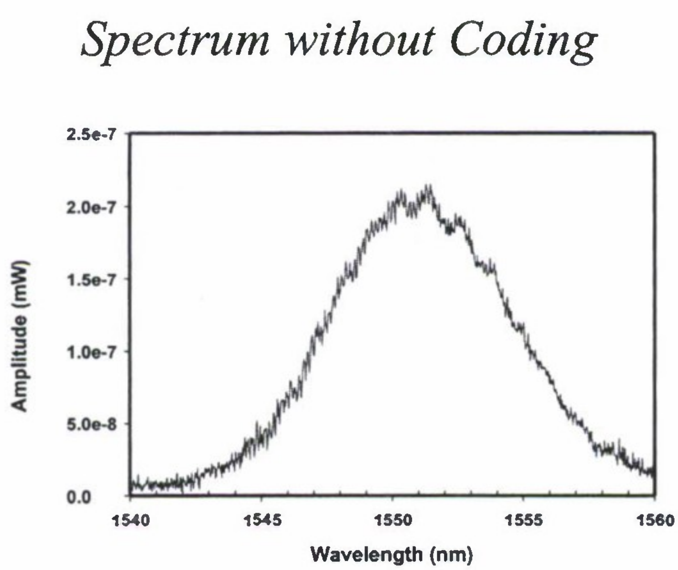


Figure 2. Power spectrum of femtosecond laser pulse used for data transmission in OCDMA experiment. Specturm shown with no coding applied.

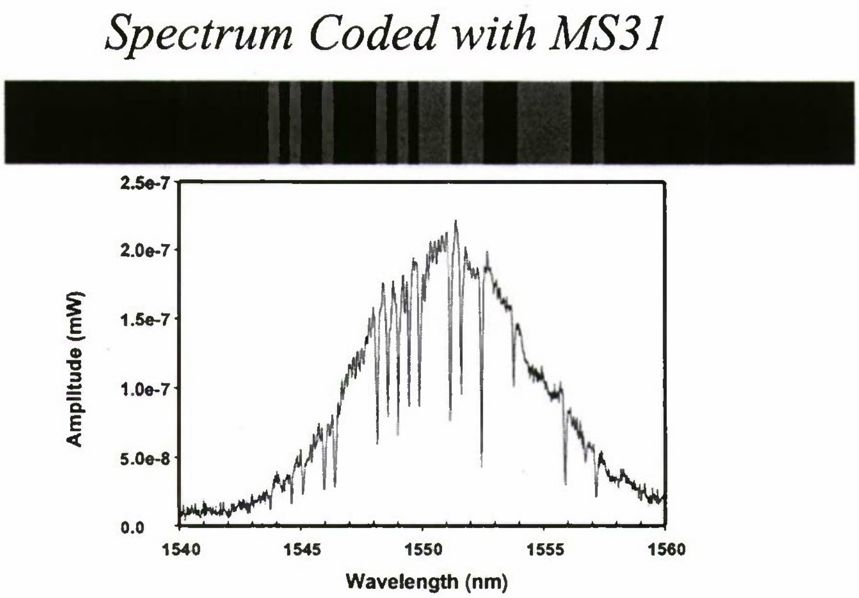


Figure 3. Power spectrum of femtosecond laser pulse used for data transmission in OCDMA experiment. Specturm shown with 31-bit M-sequence code applied. Green bars above spectrum indicate chips receiving π radians phase shift.

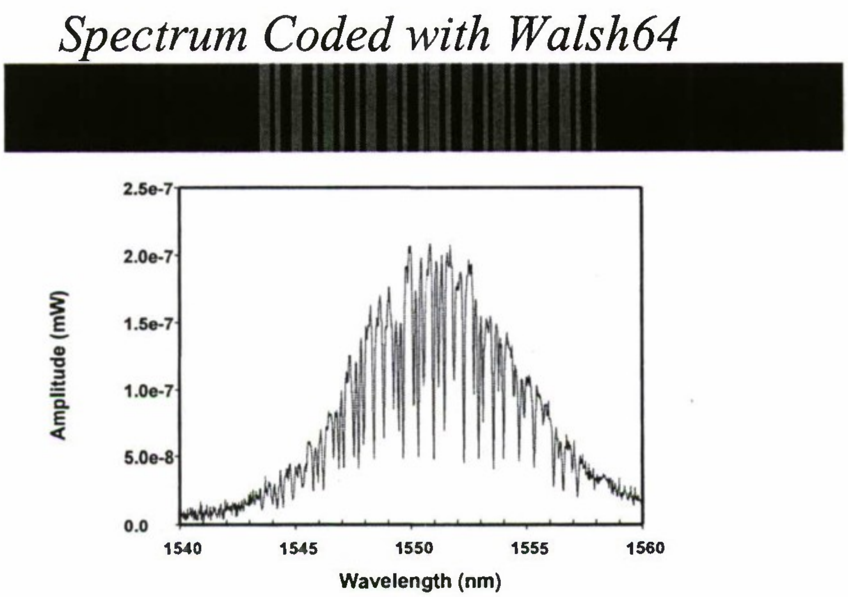


Figure 4. Power spectrum of femtosecond laser pulse used for data transmission in OCDMA experiment. Specturm shown with 64-bit Walsh code applied. Green bars above spectrum indicate chips receiving π radians phase shift.

SPECTS O-CDMA Testbed

A substantial portion of the effort of the O-CDMA group is devoted to the demonstration of a communications system based on a testbed setup of the O-CDMA principles. This is a logical and important step in the progression toward and all-integrated optical system. It allows for the development of detection and coding schemes to maximize the communications effectiveness of O-CDMA. At the same time, it forms the basis for trying out new approaches in secure communications. We now look in a little more detail at some of the technical accomplishments of the last year.

The O-CDMA testbed has become quite complicated as we have added more users. In addition, to further the goal of obtaining high spectral efficiency and yet maintaining a reasonable cost-savings in optical hardware we have implemented time gating technologies which adds a layer of discrimination on top of the spectral CDMA decoding already being performed. The time gating also improves the operation of the nonlinear thresholder at the receiver by excluding optical energy from incorrectly decoded users.

Figures 5 and 6 show a schematic diagram of the current testbed setup. The two-dimensional encoder/decoder supports 5 simultaneous optical signals as described above. In Figure 5 we see that 4 of the channels are used to encoded pulses and one channel is used as a decoder. The decoder channel contains the complex conjugate of one of the encoder channels and thus is the matched filter. Without any time-multiplexing this would be a system composed of 5 users; an "intended" transmitter and receiver and three interferers. However, by employing a time delay earlier in the system, two sequential pulses arrive at the 2D encoder array generating an additional 1 user plus 3 interferers. Thus, the system is now supporting two users (plus one redundant transmitter) and 6 interferers, or 8 total users. In order to select the correct decoded pulse from the time-multiplexed pair, we need to use a time gate as shown in Figure 6. We investigated several new technologies and found that the Nonlinear Optical Loop Mirror (NOLM) provided the best performance. The details of how this optical circuit works will not be provided here but it is sufficient to note that the gate uses a femtosecond control pulse to select the correctly decoded pulse from the multiplexed pair coming from the decoder. Figure 7 shows measurements of the effectiveness of the NOLM. The top figure shows the input to the NOLM; a combination of 8 users divided into two adjacent time slots. The boundary of each time slot is at +/-25 ps, +/-75ps, etc. Thus, we see correctly decoded pulses at the center of each time slot along with background noise corresponding to the optical energy of incorrectly decoded pulses. At the output of the NOLM only the pulse that was selected by the control pulse is visible at 0 ps. Notice the very effective reduction in background noise and the virtual elimination of the pulses in the adjacent slots. Following the NOLM is a highly nonlinear thresholder that allows detection of only the correctly decoded pulses. This device was described in last year's report.

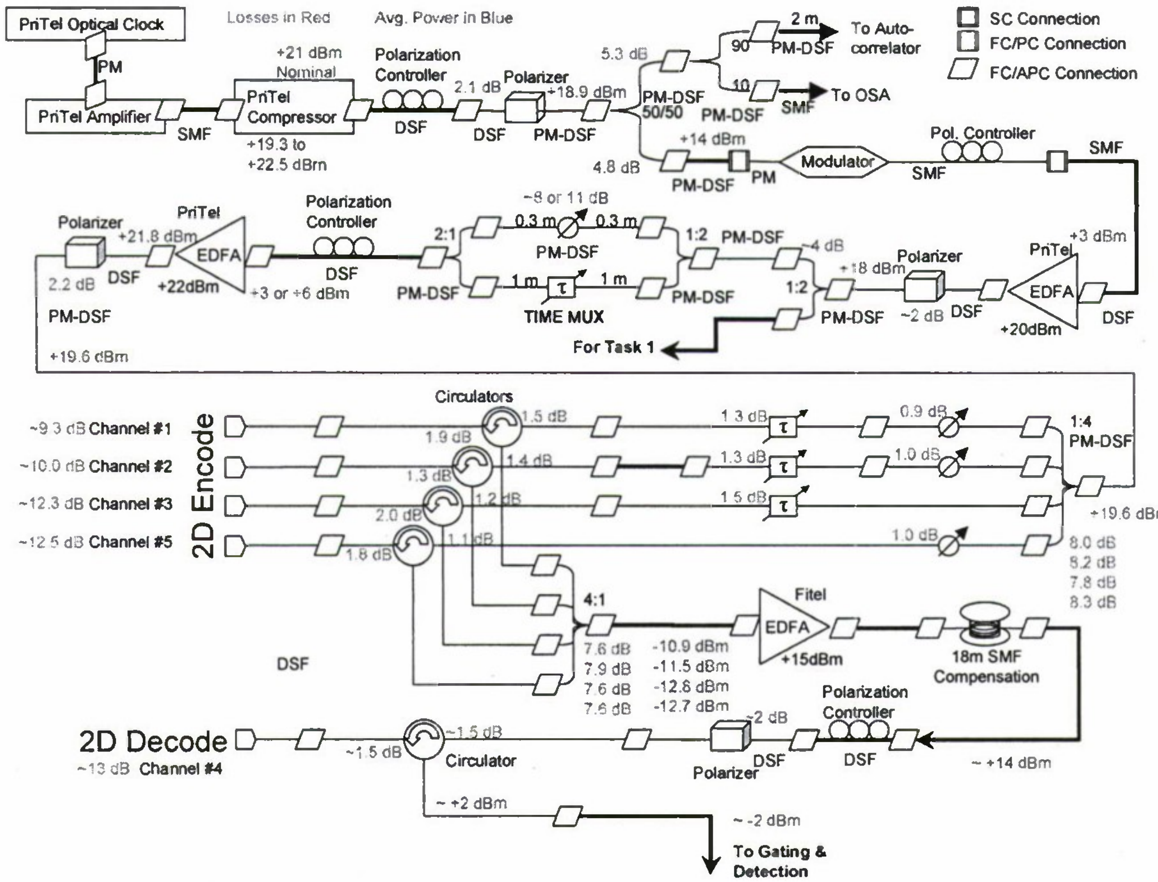


Figure 5. Detailed diagram of the eight-user SPECTS O-CDMA testbed. (Part 1)

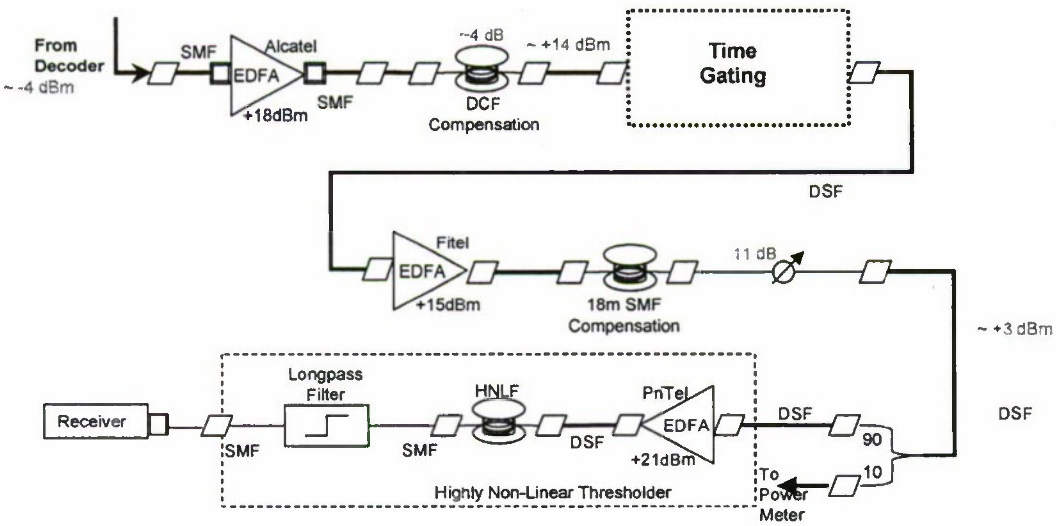
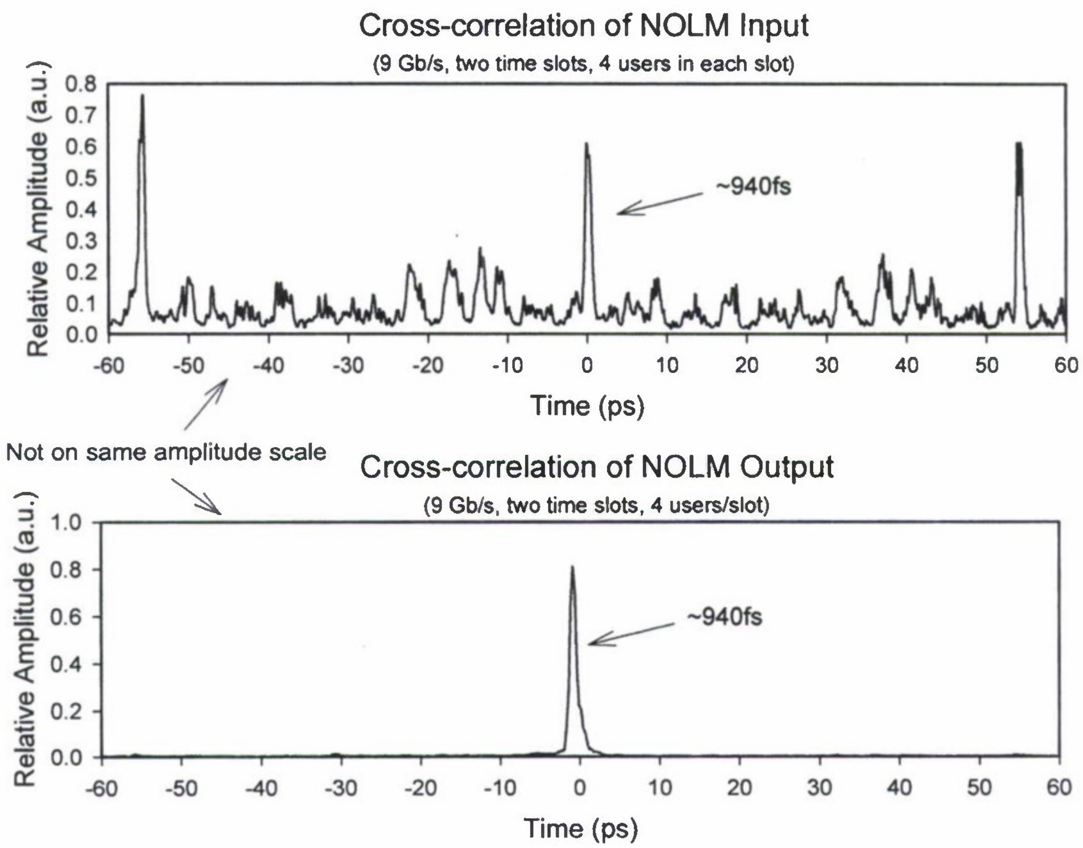


Figure 6. Detailed diagram of the eight-user SPECTS O-CDMA testbed. (Part 2)



Fugure 7. Cross-correlations showing the gating performance of the NOLM. The top figure shows the input to the NOLM (eight users, four users in each time slot). The lower figure shows the NOLM output with nearly complete suppression of the interferers and the second time slot.

BER Results for 8 Users at 9 GB/s in the NOLM-gated Testbed

BER measurements of the NOLM gated, eight-user, time-slotted O-CDMA testbed.
running at 9 GB/s were made and the data are shown in 8. Trace A is the back-to-back BER curve taken without encoders and decoder. Trace B is the BER curve with two users in the testbed (distributed in two time slots on one channel). For traces C-E, we add successive pairs of interferers. The BER curves are taken versus the total received power at the thresholder input.

We see a very small (~1 dB) power penalty between traces A and B. This is much different from previous BER measurements with our non-time-gated testbed. Normally, we would see a 4-5 dB power penalty when comparing back to back and a single user going through the encoder and decoder. This results from the spectral narrowing that occurs as the pulses go through the encoder/decoder combination. Apparently the temporal broadening that the pulse experiences through the NOLM is significant enough to hide the usual effect. As additional users are added we can see that there is a significant (6-10 dB) power penalty associated with the multi-user interference (MUI). Also, when we increase the number of users, power sharing in the saturated EDFAs before the NOLM gate decreases the total input power from the intended user channel and this will decrease the signal-to-noise ratio at the output of NOLM.

When we make a BER measurement, we keep the output power of the thresholder EDFA constant. This is different than non-gated testbeds where it is necessary to have adaptive control of the thresholder EDFA output power. We can keep the thresholder EDFA output power constant since the NOLM selects

only a 2-3 ps window out of the desired time slot and rejects most of the interfering users' power that is present outside this window.

For the back-to-back, two- and four-user cases, we achieved error-free performance. For six users, we have a BER ~ 10^{-12}, and for eight users, we have achieved BER < 10^{-9}. During the next quarter, we will continue to work on optimizing the NOLM (possibly by changing EDFAs, nonlinear fiber, etc.) to achieve error-free performance for the eight-user testbed.

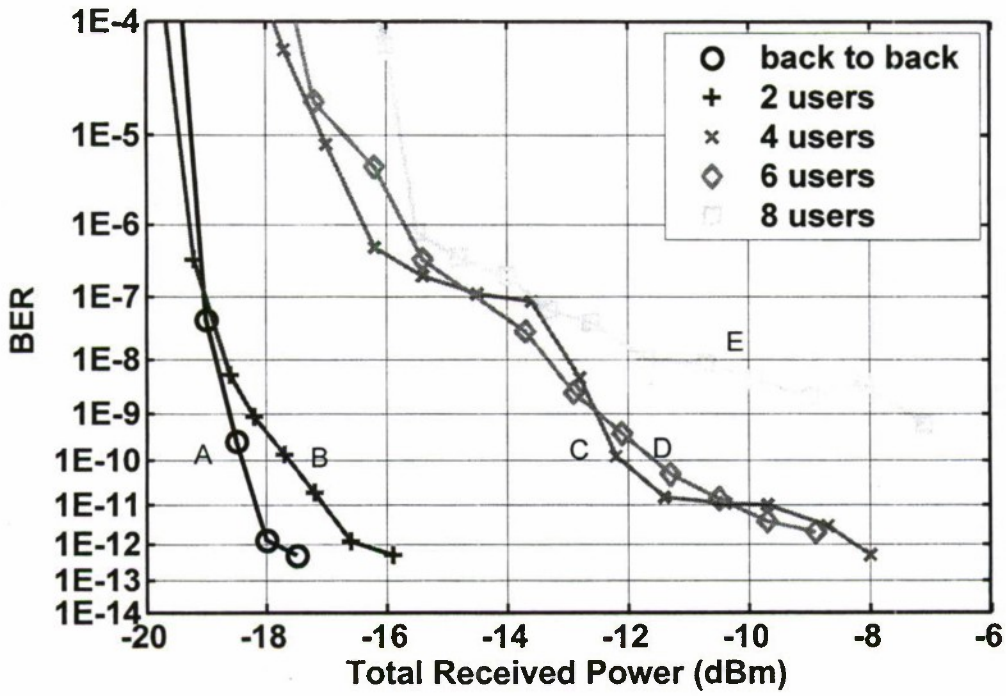


Figure 8. BER performance of the eight-user time-slotted O-CDMA testbed operating at a data rate of 9 GB/s. Total received power is measured at the input to the nonlinear thresholder.

Future Work and Prospects for Applying O-CDMA to Secure Communications

The principle of Code-Division-Multiple-Access applied in the wavelength domain is an attractive venue for applying secure communications techniques. An eavesdropper listening in on an O-CDMA channel without prior knowledge of which particular orthogonal code group is being used must search with exponential time to decipher a message. With prior knowledge this drops to a linear search time. However, our optical coding technology allows for the fairly rapid change of code group by merely changing the phase mask in the wavelength-domain modulator. In the testbed setup, our 2D LC- SLPM can only be changed on the time scale of 1 second but a large fraction of the project team is devoted to developing an all-integrated optical version of the O-CDMA in the indium-phosphide system. With this technology, we will be able to change the phase codes on a sub-microsecond time scale (perhaps to the nanosecond scale).

This would allow for altering the code on almost a bit-by-bit basis. This additional degree of freedom would render the technique virtually unbreakable by an eavesdropper. In the next two years as we further develop this technology we plan to explore this and similar ideas to produce a robust and second digital communications strategy.

Student Participation and Publications

Two students have received substantial support from this AFOSR Center for Digital Security Project. By far the most effective and influential has been Ryan P. Scott who has taken over from a post-doctoral student who left recently to join industry. Another newer student, Wei Cong, has also been indispensable in moving the testbed project forward. We are grateful to the AFOSR for their continued support.

Publications and presentations related to this work:

R. P. Scott, W. Cong, K. Li, V. J. Hernandez, J. P. Heritage, B. H. Kolner, and S. J. B. Yoo, "Demonstration of an Error-Free 4 \times10 Gb/s Multiuser SPECTS O-CDMA Network Testbed," *IEEE Photonics Technology Letters*, vol. 16, pp. 2186-88, 2004.

V. J. Hernandez, Y. Du, W. Cong, R. P. Scott, K. Li, J. P. Heritage, Z. Ding, B. H. Kolner, S. J. B. Yoo, "Spectral Phase Encoded Time Spreading (SPECTS) Optical Code Division Multiple Access for Terabit Optical Access Networks," *IEEE Journal of Lightwave Technology*, vol. 22, no. 11, 2004 (to be published).

W. Cong, R. P. Scott, V. J. Hernandez, K. Li, J. P. Heritage, B. H. Kolner, and S. J. B. Yoo, "High performance 70 Gb/s SPECTS optical-CDMA network testbed," *IEE Electronics Letters*, to be published in next issue.

K. Li, W. Cong, V. J. Hernandez, R. P. Scott, J. Cao, Y. Du, J. P. Heritage, B. H. Kolner, and S. J. B. Yoo, "10 Gbit/s optical CDMA encoder-decoder BER performance using HNLF thresholder," presented at Optical Fiber Communications Conference (OFC 2004), 2004. Paper MF87.

W. Cong, V. J. Hernandez, R. P. Scott, K. Li, J. P. Heritage, B. H. Kolner, Z. Ding, and S. J. B. Yoo, "Performance of a 10 Gb/s Optical Code Division Multiple Access Channel in the Presence of an Interferer," presented at Conference on Lasers and Electro-Optics (CLEO 2004), 2004. Paper CWH1.

Wei Cong, Ryan P. Scott, Vincent J. Hernandez, Kebin Li, Brian H. Kolner, Jonathan P. Heritage and S. J. Ben Yoo, "Demonstration of a 6 × 10 Gb/s Multiuser Time-slotted SPECTS O-CDMA Network Testbed," *Optical Fiber Communications Conference (OFC 2005)*, Submitted for review.

Vincent J. Hernandez, Wei Cong, Ryan P. Scott, Kebin Li, Jonathan P. Heritage, Brian H. Kolner and S. J. Ben Yoo, "A Synchronous O-CDMA System Incorporating UNI-based Time Gating," *Optical Fiber Communications Conference (OFC 2005)*, Submitted for review.

CDS

Network Interdiction Project; 2005 report

Personnel:

Prof. David L. Woodruff, Ph.D.

Collaborating with:

Harald Held, Dipl. Math
Raymond Hemmecke, PhD
R. Kevin Wood, PhD

Recent Advances:

We are exploring optimized interdiction of networks where the either the characteristics of the network itself or the effect of interdiction efforts cannot be known with certainty in advance. These models add important realism for networks where the characteristics of the network or the interdiction cannot be known completely in advance but rather interdiction must be planned based on conjectured configurations. In some mutli-stage formulations, we model the fact that attacking the network may result in resolving some of the uncertainty. This is particularly relevant for communication and computer networks, but also has relevance for transportation or terrorist networks.

Plan for Future Work:

Our main research thrust will be computational. We working with R. Kevin Wood of the Naval Postgraduate School and we are testing and improving methods that can solve these problems in seconds. This is obviously valuable when the methods are used in a decision support system (DSS) for planning attacks. This is perhaps even more important when used in a DSS to plan defense, since the interdiction problems must be solved repeatedly. We are also beginning to explore abstract models that could have application to the communications infrastructure associated with air defense networks.

Paper Published:

Held, H, R. Hemmecke, and D.L. Woodruff, "A Decomposition Algorithm for Planning the Interdiction of Stochastic Networks," *Naval Research Logistics*, 52 (2005), 321-328.

We describe a decomposition based solution method for a new, important class of network interdiction problems. The problem of maximizing the probability of sufficient disruption of the flow of information or goods in a network whose characteristics are not certain is shown to be solved effectively by applying a scenario decomposition method developed by Schultz. Computational results demonstrate the effectiveness of the algorithm and design decisions that result in speed improvements.

Paper In Press:

2. Held, H. and Woodruff, D.L., "Multi-stage Interdiction of Stochastic Networks," Accepted by *Journal of Heuristics*.

We describe and compare heuristic solution methods for a multi-stage stochastic network interdiction problem. The problem is to maximize the probability of sufficient disruption of the flow of information or goods in a network whose characteristics are not certain.
In this formulation, interdiction subject to a budget constraint is followed by operation of the network, which is then followed by a second interdiction subject to a second budget constraint. Computational results demonstrate and compare the effectiveness of heuristic algorithms.

Intrusion Detection Project
Rao Vemuri

Accomplishments.

1. We demonstrated that (a) robust support vector machines are far superior to the k-nearest neighbor method with the stahdard distance metric in intrusion detection and (b) a k-nearest neighbor method with a modified cosine metric is as good as the robust SVM with much less conceptual and computational difficulty.

2. We demonstrated that evolving connectionist models can capture changing user profiles, thus making them suitable for detecting insider threats.

3. We demonstrated that the "Programming Language S and Environment" - developed for statistical applications - rivals MATLAB and Mathematica while solving problems in computer secuity. Indeed, the environment provided by S makes it very easy not only to solve intrusion-related problems but also provides a powerful vehicle for visualization of the intrusion phenomenon.

4. On-going thrust is to re-examine the issues related to intrusion detection from the point of view of complexity analysis and computational learning theory (COLT).

Personnel who worked on the project

Rao Vemuri - recd. some travel support, but no salary
Yihua Liao - supported with funds
Khaled Labib - did not receive any funds, but worked with me

Publications

Khaled Labib and V. Rao Vemuri, "Anomaly Detection Using S Language Framework: Clustering and Visualization of Intrusive Attacks on Computer Systems," IEEE Security and Privacy (submitted).

Vemuri, V. and V. Sreeharirao, (Eds.), Enhancing Computer Security with Smart Technology, CRC Press, 2004. (in print)

Khaled Labib and V. Rao Vemuri, "Detecting and Visualizing Denial of Service And Network Probe Attacks Using Principal Component Analysis," SAR'04 the 3rd Conference on Security and Network Architectures, La Londe, Cote d'Azur (France), June 21-25, 2004

Rawat, Sanjay, Arun K. Pujari, V. P. Gulati, V. Rao Vemuri, "Intrusion Detection using Text Processing Techniques with a Binary-Weighted Cosine Metric," International Journal of Information Security, Springer-Verlag, Submitted 2004.

Liao, Yihua and V. Rao Vemuri and Alejandro Pasos, "A General Framework for Adaptive Anomaly Detection with Evolving Connectionist Systems", SIAM International Conference on Data Mining, Lake Buena Vista, FL, April 22-24, 2004.